UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/755,450	01/13/2004	Igor Garrievich Muttik	03.047.01	1086

7590 11/01/2007

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
SANDOVAL, KRISTIN D	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/755,450	MUTTIK, IGOR GARRIEVICH	
	Examiner	Art Unit	
	Kristin D. Sandoval	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 August 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-53 are pending.

Drawings

2. The drawings were received on August 22, 2007. These drawings are accepted

Response to Arguments

3. Applicant's arguments filed August 22, 2007 have been fully considered but they are not persuasive.

Applicant asserts that the limitation, "more strongly", in claims 1, 7, 18, 24, 35 and 41, refers to being more strongly associated than without the modifications. However, that is not clear from the claim language. The limitation states, "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" and it is not clear that the external program calls are more strongly associated with malicious computer program activity as compared to without the modifications. It could be more strongly associated with malicious computer program activity than the primary set of external program calls. Therefore the scope of "more strongly" cannot be ascertained.

Applicant further argues that Made fails to teach secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls. The examiner respectfully disagrees. Made discloses pattern identifying code that can identify program calls

associated with malicious activity and are also associated with another set of program calls such as ones that are content destructive since these calls are calls that are made as a result of the first set of calls detected by patterns (6:43-63).

Applicant further argues that Made fails to teach modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity. The examiner respectfully disagrees. Made discloses modifying the behavior patterns as new malicious behavior is detected and as more malicious behavior is detected it associated the patterns and the calls that fall within the pattern more closely with the malicious activity (6:25-43).

Applicant finally argues that Made fails to teach doing a validity check on the modified rules to verify if they are more effectively detecting malicious activity. The examiner respectfully disagrees. Made discloses a test on a prototype that analyzed the validity of the rules and Made discloses that validity is checked when patterns are detected in order to ensure no false alarms (10:52-11:7).

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 2, 8-10, 13, 14, 17, 18, 19, 25-27, 30, 34, 35, 36, 42-44, 47, 48 and 51-53 rejected under 35 U.S.C. 102(e) as being anticipated by van der Made (Made), U.S. Patent No. 7,093,239.

As per claims 1, 2, 18, 17, 35 and 36:

Made discloses a computer program product operable to detect malicious computer program activity, comprising:

logging code operable to log a stream of external program calls (10:18-29);

primary set identifying code operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls; and

modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity (6:12-24 and 11:46-60)

wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls (6:12-24).

As per claims 8-10, 25-27 and 42-22:

Made discloses a computer program product wherein said set of rules include at least one of: one or more pattern matching rules; and one or more regular expression rules, wherein said set of rules are responsive to ordering of external program calls and said modifying code dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity (5:16-39).

As per claims 13, 30 and 47:

Made discloses a computer program product wherein said stream of external program calls are logged following emulation of execution of a computer program (5:16-39).

As per claims 14, 31 and 48:

Made discloses a computer program product wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules (11:46-59).

As per claims 17, 34 and 51:

Made discloses a computer program product wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity (12:26-41).

As per claims 52-53:

Made discloses a computer program product further comprising applying high level rules to the modified set of rules, and promoting said modified set of rules from a temporary set to a permanent set based on the application of the high level rules to the modified set of rules and on the determination that the modified set of rules decreased malicious traffic (10:18-11:23, 12:26-41).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 3-5, 20-22 and 37-39 rejected under 35 U.S.C. 103(a) as being unpatentable over Made, U.S. Patent No. 7,093,239 as applied to claims 1, 18 and 35 above and further in view of Khazan et al. (Khazan), U.S. PG-PUB 2005/0108562.

As per claims 3, 20 and 37:

Khazan substantially teaches a computer program product wherein said external program calls are application program interface calls to an operating system (paragraph 0042).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the invention of Khazan in combination with the invention of Made because executing the malicious code detector of Khazan in a simulation mode would allow the executables being tested to display the malicious code symptoms without actually hurting the computer system it resides on as taught by Khazan (paragraph 0111).

As per claims 4, 5, 21, 22, 38 and 39:

Khazan substantially teaches a computer program product wherein each of said external program calls has one or more characteristics compared against said set of rules, wherein said one or more characteristics include: a call name; a return address; one or more parameter values; and one or more returned results (paragraph 0042).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the invention of Khazan in combination with the invention of Made because executing the malicious code detector of Khazan in a simulation mode would allow the executables being tested to display the malicious code symptoms without actually hurting the computer system it resides on as taught by Khazan (paragraph 0111).

2. Claims 6-7, 23-24 and 40-41 rejected under 35 U.S.C. 103(a) as being unpatentable over Made as applied to claims 1, 18 and 35 above, and further in view of Obrecth et al. (Obrecht), U.S. PG-PUB 2004/0064736.

As per claims 6-7, 23-24 and 40-41:

Obrecht substantially teaches a computer program product wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level and the score level associated with the secondary set is increased to more strongly associate the secondary set with malicious program activity (paragraph 0039).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the score and weight system of Obrecht with the emulation system of Made in order to create a more robust computer system as taught by Obrecht (paragraph 0056).

3. Claims 11-12, 28-29 and 45-46 rejected under 35 U.S.C. 103(a) as being unpatentable over Made as applied to claim 1, 18 and 35 above, and further in view of Judge, U.S. Patent No. 7,096,498.

As per claims 11-12, 28-29 and 45-46:

Judge substantially teaches a computer program product wherein at least changes within said set of rules are transmitted to one or more remote computer such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity (abstract) and to a rules supplier (20:5-34).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to propagate the rules to other systems in order to get a global view of traffic patterns as disclosed in Judge (6:58-7:10).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin D Sandoval
Examiner
Art Unit 2132

KDS

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100